

1 NICOLA T. HANNA
United States Attorney
2 LAWRENCE S. MIDDLETON
Assistant United States Attorney
3 Chief, Criminal Division
RYAN H. WEINSTEIN (Cal. Bar No. 240405)
4 Assistant United States Attorney
OCDETF Section
5 1400 United States Courthouse
312 North Spring Street
6 Los Angeles, California 90012
Telephone: (213) 894-8957
7 Facsimile: (213) 894-0142
E-mail: ryan.weinstein@usdoj.gov

8 Attorneys for Applicant
9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT
11
12 FOR THE CENTRAL DISTRICT OF CALIFORNIA

13 IN THE MATTER OF THE SEARCH
OF A RED IPHONE SEIZED ON
14 JUNE 21, 2018, AND MAINTAINED
IN THE CUSTODY OF THE DRUG
ENFORCEMENT ADMINISTRATION

No. 2:18-MJ-01833

GOVERNMENT'S EX PARTE APPLICATION
FOR FIRST EXTENSION OF TIME WITHIN
WHICH TO RETAIN AND SEARCH
ENCRYPTED DIGITAL DEVICE AND DATA;
DECLARATION OF RYAN H. WEINSTEIN

(UNDER SEAL)

20 The United States of America, by and through its counsel of
21 record, Assistant United States Attorney Ryan H. Weinstein, hereby
22 applies for an order extending by 180 days the time within which the
23 government may retain and continue to attempt to search an encrypted
24 digital device and data, seized pursuant to a federal search
25 warrant.

26 //
27
28

1 This application is based on the attached declaration of Ryan
2 H. Weinstein and the files and records of this case, including the
3 underlying search warrant and affidavit in support thereof, the
4 search warrant and affidavit in CR Misc. No. 2:18-MJ-01605 and any
5 previously filed applications for extensions.

6 Dated: December 7, 2018

Respectfully submitted,

7 NICOLA T. HANNA
8 United States Attorney

9 LAWRENCE S. MIDDLETON
10 Assistant United States Attorney
11 Chief, Criminal Division



12

RYAN H. WEINSTEIN
13 Assistant United States Attorney

14 Attorneys for Applicant
15 UNITED STATES OF AMERICA
16
17
18
19
20
21
22
23
24
25
26
27
28

DECLARATION OF RYAN H. WEINSTEIN

I, Ryan H. Weinstein, hereby declare and state:

1. I am an Assistant United States Attorney assigned to this investigation for United States Attorney's Office for the Central District of California.

2. This declaration is made in support of a request for an order permitting the government to retain and search the following digital device and data, seized pursuant to a previously authorized search warrant, which is encrypted or which contains encrypted files:

a. a red iPhone with "iPhone PRODUCT" inscribed on the the phone, seized on June 21, 2018, and currently maintained in the custody of Drug Enforcement Administration in Los Angeles, California ("**Subject Device #1**" or the "**Subject Device**").

3. On July 17, 2018, Special Agent Jordan T. Lester of the Drug Enforcement Administration (the "Investigating Agency"), obtained a search warrant issued by the Honorable Rozella A. Oliver, United States Magistrate Judge, authorizing the search of the **Subject Device** for evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1) (Possession with the Intent to Distribute a Controlled Substance), 846 (Conspiracy to Distribute a Controlled Substance), and 848(e) (Murder in Furtherance of a Drug-Trafficking Crime), and Title 18, United States Code, Section 1958 (Use of Interstate Commerce Facilities in the Commission of Murder-for-Hire) (the "Subject Offenses"). The **Subject Device** had been seized pursuant to a separate warrant, issued by the Honorable Patrick J. Walsh, United States Magistrate Judge, in CR Misc. No. 2:18-MJ-01605.

1 4. Based on information obtained from Special Agent Flanigan,
2 I learned the following:

3 a. On or about July 21, 2018, agents from the
4 Investigating Agency executed the warrant. Thus far, the
5 Investigating Agency has been unable to begin its search of the
6 **Subject Device** because the Investigating Agency has been unable to
7 bypass the **Subject Device's** security and encryption features. The
8 **Subject Device** is protected by a six-digit password. Technicians
9 are currently attempting to overcome the **Subject Device's** security
10 features using the so-called "brute force" method, which involves
11 the use of a computer to systematically attempt every possible
12 password combination. This process can take several months to
13 complete.

14 5. Although investigators cannot currently bypass the
15 encryption on the device described above, I know that new methods
16 for bypassing encryption and for decrypting files and devices are
17 constantly being developed. In addition, I know that it is not
18 uncommon for passwords to be discovered or learned as an
19 investigation continues, for example when witnesses cooperate, when
20 additional locations are searched, or during ongoing review of
21 seized electronic data. Therefore, I seek permission for the
22 government to retain the device/data described above, and to
23 continue to attempt to access them, in the event that such methods
24 or information are developed or discovered and the device/data can
25 be unlocked or otherwise accessed.

26 6. I believe the device is likely to contain, or to be,
27 evidence, fruits, or instrumentalities of the Subject Offenses for
28

1 the reasons stated in the affidavit in support of the underlying
2 warrant in this matter.

3 7. Because there remains probable cause to believe that the
4 device at issue contains evidence, fruits, or instrumentalities of
5 the offense(s) described in the underlying warrant, the government
6 seeks to retain the device identified in this application for a
7 further period of 180 days past the end of the currently authorized
8 search period, in order to continue to attempt to bypass the
9 decryption and search the device/files. During this period, the
10 government may continue to attempt to search the device if new
11 technology is obtained or if potential passwords for the device or
12 files are located during the investigation.

13 8. If the government continues to be unable to access the
14 device/files for a period of 90 days, it will file a status report
15 to the court, stating that it has not been able to access the
16 device/files. If the government is able to access the device or
17 files, it will promptly file a report so notifying the court with
18 the date(s) of access and will follow the search protocols set forth
19 in the original warrant.

20 I declare under penalty of perjury that the foregoing is true
21 and correct to the best of my knowledge and belief.

22 DATED: December 7, 2018

23 
24 RYAN H. WEINSTEIN